INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/052445

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99/43120 A (DIGITAL VIDEO EXPRESS L P ;KRAVITZ DAVID W (US); GOLDSCHLAG DAVID) 26 August 1999 (1999-08-26) abstract page 23, line 10 - page 34, line 10	1-22
Y	WO 91/11884 A (SCIENTIFIC ATLANTA) 8 August 1991 (1991-08-08) cited in the application page 12 page 18 - page 19	1-22

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 January 2005	03/02/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Bertrand, F

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/052445

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	MENEZES A ET AL: "HANDBOOK OF APPLIED CRYPTOGRAPHY, PUBLIC-KEY ENCRYPTION" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 294-297,285-287,524-525, XP002272612 ISBN: 0-8493-8523-7 the whole document	1-22
A	EP 0 658 054 A (NEWS DATACOM LTD) 14 June 1995 (1995-06-14) the whole document	1-22
A	WO 99/18729 A (BENARDEAU CHRISTIAN ;CANAL PLUS SA (FR); MAILLARD MICHEL (FR); DAU) 15 April 1999 (1999-04-15) abstract page 23, line 10 - page 34, line 10	1-22
A	DESMEDT Y G: "THRESHOLD CRYPTOGRAPHY" EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS AND RELATED TECHNOLOGIES, AEI, MILANO, IT, vol. 5, no. 4, 1 July 1994 (1994-07-01), pages 35-43, XP000460560 ISSN: 1120-3862 the whole document	7-10
A	BONEH D ET AL: "EFFICIENT GENERATION OF SHARED RSA KEYS" ADVANCES IN CRYPTOLOGY - CRYPTO '97. SANTA BARBARA, AUG. 17 - 21, 1997, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO), BERLIN, SPRINGER, DE, vol. CONF. 17, 17 August 1997 (1997-08-17), pages 425-439, XP000767548 ISBN: 3-540-63384-7 the whole document	7-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/052445

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9943120	A	26-08-1999	AU	2766599 A	06-09-1999
			CA	2319538 A1	26-08-1999
			EP	1057299 A1	06-12-2000
			TW	432852 B	01-05-2001
			WO	9943120 A1	26-08-1999
			ZA	9901362 A	20-08-1999
			WO	9953689 A1	21-10-1999
			US	6738905 B1	18-05-2004
WO 9111884	A	08-08-1991	US	5029207 A	02-07-1991
			AR	246145 A1	30-03-1994
			AT	180936 T	15-06-1999
			AT	192891 T	15-05-2000
			AU	635180 B2	11-03-1993
			AU	7340291 A	21-08-1991
			BR	9104261 A	03-03-1992
			CA	2049310 A1	02-08-1991
			DE	69131285 D1	08-07-1999
			DE	69131285 T2	30-09-1999
			DE	69132198 D1	15-06-2000
			DE	69132198 T2	23-11-2000
			EP	0466916 A1	22-01-1992
			EP	0809402 A1	26-11-1997
			JP	4506736 T	19-11-1992
			JP	3304084 B2	22-07-2002
			MX	172416 B	15-12-1993
			WO	9111884 A1	08-08-1991
			US	5237610 A	17-08-1993
EP 0658054	A	14-06-1995	IL	107967 A	05-12-1996
			AT	171331 T	15-10-1998
			AU	684112 B2	04-12-1997
			AU	8034294 A	15-06-1995
			CA	2137608 A1	10-06-1995
			DE	69413361 D1	22-10-1998
			EP	0658054 A2	14-06-1995
			HK	1012811 A1	12-05-2000
			JP	7288522 A	31-10-1995
			US	5590200 A	31-12-1996
WO 9918729	A	15-04-1999	AT	273597 T	15-08-2004
			AU	748518 B2	06-06-2002
			AU	9278298 A	27-04-1999
			BR	9812703 A	22-08-2000
			CA	2305644 A1	15-04-1999
			CN	1280742 T	17-01-2001
			DE	69825611 D1	16-09-2004
			EP	1020080 A1	19-07-2000
			HR	20000165 A1	30-04-2001
			HU	0100232 A2	28-05-2001
			WO	9918729 A1	15-04-1999
			ID	23916 A	25-05-2000
			JP	2001519629 T	23-10-2001
			NO	20001649 A	02-06-2000
			PL	339572 A1	18-12-2000
			TR	200001560 T2	21-12-2000
			ZA	9808951 A	12-04-1999